ISSN 2181-3187

AXBOROT TEXNOLOGIYANI BOSHQARISH XAVFSIZLIGI VOSITALARI

Suyarov A.M.
Samarqand iqtisodiyot
va servis instituti dotsenti
akramsuyarov@mail.ru

Qo'ziboyeva R.F.
Samarqand davlat universiteti
Urgut filiali Biznesni boshqarish
va tabiiy fanlar fakulteti 3-bosqich talabasi
ruxshonafarhodovna37@gmail.com

Annotatsiya. Zamonaviy tashkilotlar axborot texnologiyalariga (AT) tobora ko'proq tayanar ekan, axborot xavfsizligini ta'minlash dolzarb ahamiyat kasb etmoqda. AT boshqaruvida xavfsizlikni ta'minlash uchun turli xil vositalar va texnologiyalar qo'llaniladi. Ushbu maqolada tashkilotlar tomonidan qo'llaniladigan eng keng tarqalgan xavfsizlik vositalari va ularning vazifalari haqida so'z boradi.

Tayanch so'zlar: devor, shubhali xatti-harakatlar, ruxsatsiz kirish, elektron pochta, xavfsizlik qatlami, imtiyozli foydalanuvchi.

1. Tarmoq xavfsizligi vositalari.

Firewall (Devor). Tarmoqqa kiruvchi va tarmoqdan chiquvchi trafikni nazorat qiladi. Ruxsat berilgan trafikni o'tkazadi, ruxsat etilmagan trafikni esa bloklaydi.

ISSN 2181-3187

Intrusion Detection and Prevention Systems (IDPS - Hujum aniqlash va oldini olish Tizimlari). Tarmoqdagi g'alati va shubhali xatti-harakatlarni aniqlaydi va ularga qarshi choralar ko'radi.

Virtual Private Networks (VPN - Virtual Xususiy Tarmoqlar). Internet orqali xavfsiz ulanishlarni yaratadi. Ma'lumotlarni shifrlab, maxfiylikni ta'minlaydi.

Network Access Control (NAC - Tarmoqqa kirishni boshqarish). Tarmoqqa ulangan qurilmalarni nazorat qiladi va ruxsatsiz qurilmalarning tarmoqqa kirishini oldini oladi.

Load Balancers (Yuk taqsimlagichlar). Tarmoqdagi yuklamani taqsimlab, serverlarning haddan tashqari yuklanishini oldini oladi. Bu tarmoqning ishlashini yaxshilaydi.

2. Ma'lumotlar xavfsizligi vositalari.

Data Loss Prevention (DLP - Ma'lumotlarning yo'qolishini oldini olish). Muhim ma'lumotlarning tashkilotdan tashqariga chiqib ketishini oldini oladi. Bu elektron pochta, USB drayvlar va boshqa kanallar orqali ma'lumotlar chiqishini nazorat qilishni o'z ichiga oladi.

Data Encryption (Ma'lumotlarni shifrlash). Ma'lumotlarni shifrlab, ularning ruxsatsiz foydalanuvchilar uchun o'qib bo'lmaydigan holatga keltirilishini ta'minlaydi. Ma'lumotlar saqlash va uzatish paytida shifrlanishi mumkin.

Database Security (Ma'lumotlar bazasi xavfsizligi). Ma'lumotlar bazalariga ruxsatsiz kirishni oldini olish uchun ishlatiladigan vositalar. Bu ma'lumotlarni nazorat qilish, audit qilish va shifrlashni o'z ichiga oladi.

Data Masking (Ma'lumotlarni Yashirish). Ma'lumotlarni o'zgartirib, ularning asl nusxasini maxfiy saqlaydi. Bu test qilish va rivojlantirish kabi muhitlarda muhim ma'lumotlarni himoya qilish uchun ishlatiladi.

ISSN 2181-3187

3. Identifikatsiya va kirishni boshqarish vositalari.

Multi-Factor Authentication (MFA - Ko'p Faktorli Autentifikatsiya). Kirish jarayoniga qo'shimcha xavfsizlik qatlamini qo'shadi. Bu parol, SMS-kod, biometrik ma'lumotlar va boshqa tasdiqlash usullarini o'z ichiga olishi mumkin.

Role-Based Access Control (RBAC - Rolga Asoslangan Kirishni Boshqarish). Foydalanuvchilarning rollariga qarab ularning tizim resurslariga kirishini boshqaradi. Bu tizimning xavfsizligini ta'minlashga yordam beradi.

Privileged Access Management (PAM - Imtiyozli kirishni boshqarish). Administratorlar va boshqa imtiyozli foydalanuvchilarning tizim resurslariga kirishini nazorat qiladi va ular tomonidan amalga oshirilgan harakatlarni kuzatib boradi.

Single Sign-On (SSO - Yagona kirish). Foydalanuvchilarga bir marta autentifikatsiya qilib, bir nechta dastur va xizmatlarga kirish imkonini beradi.

4. Zararli dasturlardan himoya vositalari.

Antivirus Software (Antivirus dasturlari). Viruslar, troyanlar va boshqa zararli dasturlarni aniqlaydi va yo'q qiladi.

Antimalware Software (Zararli Dasturlarga Qarshi Dasturlar). Turli xil zararli dasturlardan himoya qiladi va ularni aniqlaydi.

Endpoint Detection and Response (EDR - Xulosa Nuqtalarini Aniqlash va Javob Berish). Kompyuterlar va boshqa xulosa nuqtalaridagi zararli faoliyatni aniqlaydi va ularga tezkor javob berishga yordam beradi.

5. Boshqa vositalar.

Security Information and Event Management (SIEM - Xavfsizlik Ma'lumotlari va Voqealarni Boshqarish). Tizim va tarmoqdan olingan xavfsizlik ma'lumotlarini to'playdi, tahlil qiladi va xavfsizlik holatini monitoring qiladi.

ISSN 2181-3187

Vulnerability Scanners (Zaifliklarni Skannerlar). Tizimlar va dasturlardagi zaifliklarni aniqlaydi va ularni tuzatishga yordam beradi.

Penetration Testing (Kirib Ko'rish Testi). Tizimlar va tarmoqlarning xavfsizlik zaifliklarini aniqlash uchun kiberhujum simulyatsiyasini amalga oshiradi.

Xulosa.

Axborot texnologiyalari boshqaruvida xavfsizlikni ta'minlash uchun yuqorida ko'rsatilgan vositalar va texnologiyalardan kompleks tarzda foydalanish kerak. Tashkilotlar o'zlarining ehtiyojlariga va xavf darajasiga qarab eng mos vositalarni tanlashlari va ularni muntazam ravishda yangilab turishlari kerak. Xavfsizlikni ta'minlash faqatgina texnologiyadan foydalanish bilan cheklanib qolmay, balki xodimlarni o'qitish va xavfsizlik siyosatini joriy qilishni ham o'z ichiga olishi kerak.

Foydalanilgan adabiyotlar

1. Pressman, R. S. (2014). "Software Engineering: A Practitioner's Approach"
2. Elmasri, R., & Navathe, S. B. (2015). "Fundamentals of Database Systems"
3. Chelsea Yang (2021). Why Use Infographics for Education https://www.edrawsoft.com/infographics/why-use-infographics-foreducation.html.
4. Т. С. Масылюк. Инфографика как средство визуализации информации. Методические рекомендации. г. Добрянка, 2017 г.